Washington and Lee Law Review

Volume 57 | Issue 4 Article 6

Fall 9-1-2000

Are We Overprotecting Code? Thoughts on First-Generation Internet Law

Orin S. Kerr

Are We Overprotecting Code? Thoughts on First-Generation Internet Law

Orin S. Kerr*

This Essay argues that Internet law presently suffers from a tendency to regulate cyberspace based on form rather than function. In areas such as free speech, patent law, and privacy law, judges and legislatures have regulated Internet code based on what it is, rather than what it does. The result has been remarkably broad rules that extend far greater legal protection to code in cyberspace than its equivalents receive in the physical world. The author suggests that greater focus on function can permit more accurate applications of traditional legal doctrines to the Internet.

I. Introduction

The French artist Georges Seurat is famous for his paintings of Parisian street scenes that consist entirely of thousands of small dots.[1] If you view a Seurat painting from just a few inches away, every bit of canvas looks the same. No matter where you look, you see only colored dots. As you walk away from the painting, however, objects begin to form. The dots coalesce into distinct images of people, trees, grass, and sky. At a sufficient distance, the dots disappear altogether, and where you once saw dots you see instead a colorful landscape of late nineteenth century Paris.

---

* Associate Professor, George Washington University Law School, beginning Fall 2001. B.S.E., Princeton University; M.S., Stanford University; J.D., Harvard Law School. Trial Attorney, Computer Crime and Intellectual Property Section, United States Department of Justice, Washington, D.C. The views expressed in this Essay are mine alone and do not represent the position of the United States Department of Justice. I wish to thank Erica Hashimoto, Neal Katyal, Marc Zwillinger, Abigail Phillips, and Sara Maurizi for commenting on earlier drafts.

1. *See generally* JOHN RUSSELL, SEURAT (1965). Seurat's most famous works are a series of paintings entitled *Un Dimanche d'Été A L'ile de la Grande Jatte* (1884-85) ("A Sunday in the Summer of the Isle of the Grande Jatte"), which portray wealthy Parisians strolling in a park along a river.

Like a Seurat painting, the Internet has both a "close-up" version and a very different version at a distance. Close up, the Internet consists of a web of networked computers that process billions of electronic instructions consisting entirely of digital 0's and 1's. This perspective is like Seurat's dots: No matter where you look, every type of communication and instruction is exactly the same. Everything on the Internet is code, an algorithm, a series of inputs and outputs.[2] Step back, however, and the Internet changes. From a distance, the 0's and 1's of the Internet resolve into the distinct and varied contents that define our understanding of the virtual world of cyberspace. The 0's and 1's transform into personal letters, commercial advertisements, hate speech, pornography, political commentary, shopping excursions, free music, malicious computer viruses, and everything else you can find online. Like Seurat's dots, the code fades from view and is replaced by the full picture of life in cyberspace.

In this Essay, I will argue that Internet law presently suffers from a tendency to adopt the close-up view of the Internet, and that this tendency has distorted the application of traditional legal doctrines to computers and the Internet. In contexts ranging from the First Amendment and privacy law to patent law, the law of the Internet has regulated code based on its form, not its function. Like museumgoers eyeing a Seurat painting from inches away, judges and legislators have viewed Internet code and communications as 0's and 1's zipping around the world, without much consideration of what the 0's and 1's are there to do. This failure to appreciate code as a backdrop to the virtual world of cyberspace has led courts to embrace an Internet formalism characterized by broad rules that apply equally to all code regardless of its contents. In short, Internet law tends to regulate code based on what the code *is*, rather than the more nuanced conception of what the code *does*. Whereas law in the physical world distinguishes carefully between different types of algorithms, communications, and ideas, the law of cyberspace presently treats all code equally.

I will also argue in this Essay that the close-up view of the Internet has had a systematic effect on the nature and scope of Internet law. The adoption of a close-up perspective has led to the overprotection of code – a tendency to conclude that statutory and constitutional protections should apply particularly broadly in cyberspace. Our legal system traditionally affords special protections to certain types of communications and algorithms, protections

2. In this Essay, I use the term "code" to refer broadly to communications and instructions that networked computers use, follow, and share in the course of their operation. This definition includes Internet protocols, software programs and algorithms, the contents of electronic communications among Internet users, and any other type of meaningful data or data structure used by networked computers and their users. *Cf.* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 6 (1999) (using "code" to refer to "the software and hardware that make cyberspace what it is").

such as privacy from eavesdropping, First Amendment protections, and protection as intellectual property. Because Internet law tends to treat all code equally regardless of its contents, it has expanded the scope of these protections in cyberspace to include all code. The result has been a dramatic expansion of the scope of legal protection that code receives in cyberspace as compared to the physical world of "realspace." Recent decisions indicate a simple rule: if it's code, the law of cyberspace will protect it. The close-up view of the Internet has made all code look the same, which has led the courts to conclude that all code deserves protection.

I will present my argument using three examples. The first example is the Sixth Circuit's recent First Amendment decision in *Junger v. Daley*,[3] which held that all computer source code is protected speech. My second example comes from patent law, and examines the Federal Circuit's expansion of the scope of patent protection for computerized algorithms in *State Street Bank & Trust Co. v. Signature Financial Group*.[4] The third example studies the law of electronic surveillance and examines how electronic privacy laws extend unusually broad privacy protections to unauthorized users of computer networks. Quite obviously, these three areas of law are very different. In each case, however, I will argue that the law has overprotected code in the same way by regulating code based on what it is, rather than what it does. By adopting a close-up view of computers and the Internet rather than a deeper functional perspective, judges and legislators have distorted the application of law to the Internet and granted greater protection to code in cyberspace than the law extends to analogous code in realspace.

I will leave it to the reader to decide whether the effects of this distortion are good or bad for the future of the Internet. To the libertarian crowd that includes most Internet law specialists, the distortions present a mixed bag. The expansion of free speech in *Junger* is generally celebrated;[5] the expansion of patent protection in *State Street* is usually condemned.[6] My purpose is not to pass on the substantive merits of these decisions, but instead to reveal their common origins. The examples I discuss in this Essay collectively reflect first-generation efforts to apply traditional legal doctrines to the Internet. It is my hope that this Essay can help lead to a greater appreciation of the functional perspective of Internet law, which in turn may lead to a more nuanced

---

3. 209 F.3d 481, 485 (6th Cir. 2000).

4. 149 F.3d 1368, 1372 (Fed. Cir. 1998).

5. *See, e.g.*, Press Release, ACLU, *In Legal First, Federal Appeals Court Is Unanimous: First Amendment Applies to Programming Code, available at* www.aclu.org/news/2000/n040400c.html (last visited on July 20, 2000) (expressing approval for Sixth Circuit's decision in *Junger*).

6. *See, e.g.*, James Gleick, *Patently Absurd*, N.Y. TIMES MAG., Mar. 12, 2000, § 6, at 44 (criticizing *State Street*).

second generation of Internet law that will more closely match the law of cyberspace to the law of realspace.[7]

I. The First Amendment

Professor Peter Junger teaches computer law at the Case Western University Law School in Ohio. In 1997, Junger challenged the Clinton Administration's regulations on the export of encryption products by attempting to publish on the World Wide Web the source code of an encryption program he had authored.[8] When the Commerce Department denied Junger's application to publish the source code without a special license, Junger brought a civil suit claiming that the denial constituted an infringement of his First Amendment rights to free speech.[9]

The first challenge Professor Junger faced in his lawsuit was convincing the court that his encryption source code was sufficiently expressive to constitute "speech." After all, source code is simply the text of a computer program; the primary purpose of source code is to instruct a computer, not to express ideas. Professor Junger's case therefore posed a broad threshold question: is source code speech, such that regulating source code can infringe upon First Amendment freedoms?[10]

The Sixth Circuit answered with a resounding "yes." Writing for a unanimous panel, Judge Martin concluded that source code is inherently expressive because it provides a means for computer programmers to communicate amongst themselves:

> [M]uch like a mathematical or scientific formula, one can describe the function and design of encryption software with a prose explanation; however, for individuals fluent in a computer programming language, [encryp-

7. My argument shares a common thread with Tim Wu's recent essay in the *Virginia Law Review*. *See generally* Timothy Wu, *Application-Centered Internet Analysis*, 85 VA. L. REV. 1163 (1999). In his piece, Wu warns that we should not view the Internet as having a single essential "nature" because an Internet user's experience varies depending on the particular application that she uses. *Id.* at 1163-65. This Essay makes a related but antecedent point: that when we apply traditional legal doctrines to the Internet, we must first decide whether to credit the Internet user's experience at all. The close-up perspective on the Internet offers an external perspective: it sees the Internet as computers processing data, not as a virtual world of cyberspace. In contrast, the functional perspective accepts the user's internal perspective of cyberspace and attempts to match the rules of the virtual world of cyberspace with the rules of realspace. *See* H.L.A. HART, THE CONCEPT OF LAW 89-91 (2d ed. 1994) (contrasting internal and external approaches).

8. *See* Junger v. Daley, 209 F.3d 481, 482-83 (6th Cir. 2000).

9. *Id.*

10. Importantly, this threshold question does not end the matter. Even if source code is speech, its regulation may be justified if the regulation is sufficiently tailored to an important government interest. *See* Universal City Studios v. Reimerdes, 111 F. Supp. 2d 294, 329-30 (S.D.N.Y. 2000).

> tion] source code is the most efficient and precise means by which to communicate ideas about cryptography.[11]

The court concluded that "[b]ecause computer source code is an expressive means for the exchange of information and ideas about computer programming, we hold that it is protected by the First Amendment."[12] In other words, because the First Amendment protects our right to discuss how computer programs work, it also protects our right to express how those ideas work through the transmission of actual source code. Ergo, source code equals speech. Civil liberties groups cheered.[13]

But does the court's reasoning make any sense? The breadth of its holding should raise eyebrows. According to Judge Martin, the "expression" that source code communicates is information about the source code itself, and Professor Junger's encryption source code was expressive because it provided a means of sharing ideas about how to author encryption source code. But according to this reasoning, every series of computer instructions warrants First Amendment protection because code will always convey information about itself. The source code of a program that does *X* will *always* be the author's means of expressing how to write a program that does *X*, no matter what *X* actually is. For example, the source code of the destructive Love Bug computer virus that infected computers worldwide in May 2000 was the author's means of expressing how to write a particularly destructive computer virus.[14] No matter what the source code actually is or does, *Junger* indicates, its status as source code automatically entitles the code to First Amendment protection. No exceptions.

Whatever you think of the political implications of this libertarian approach, it's not hard to see that it treats cyberspace radically differently from the physical world. The problem is that *everything* is "an expressive means for the exchange of information and ideas" about itself, and this is just as true in realspace as in cyberspace. For example, imagine that you have designed a new kind of padlock, and you wish to explain to me how the lock works. The best way to communicate that set of ideas is to give me one of the locks, let me play with it, take it apart, and see for myself how it operates. Sure, you could write a book that offers "a prose explanation" for how the padlock works, but I will learn much more by examining the lock first-hand. To borrow a phrase from the *Junger* court, access to the lock itself provides "the most efficient and

---

11. *Junger*, 209 F.3d at 484.

12. *Id.* at 485.

13. *See, e.g.*, Press Release, ACLU, *In Legal First, Federal Appeals Court Is Unanimous: First Amendment Applies to Programming Code, available at* www.aclu.org/news/2000/n040400c.html (last visited on July 20, 2000) (applauding Sixth Circuit's decision in *Junger*).

14. *See* Ted Bridis, *Virus Gives "Love" a Bad Name*, WALL ST. J., May 5, 2000, at B1 (describing impact of Love Bug computer virus).

precise means by which to communicate ideas" about it. And so it is for everything else in the world. Robbing a bank provides the most instructive way to teach someone how to rob a bank; kicking someone in the shins provides an excellent way of communicating the concept of kicking someone in the shins. So long as the only "expression" we are concerned with is information about the act or thing itself, that act or thing is bound to be an "an expressive means for the exchange of information and ideas" about it.

But does this mean that you have a First Amendment right to distribute padlocks, to rob banks, and to kick people in the shins? Of course not. In the physical world, we recognize that the "expression" that the First Amendment protects goes beyond what things *are* to what they *say*.[15] Just look at the Supreme Court's cases involving expressive conduct. According to the Court, burning the American flag is protected expression – not because it provides an efficient means of communicating ideas about how to burn flags, but because it communicates a political message about the United States.[16] Similarly, spending money on a political campaign can constitute expressive speech because it furthers causes that the campaign represents, not because it gives other people ideas about how to spend money.[17] Neither burning flags nor giving money to a campaign is speech in a formal sense. However, the First Amendment protects both acts because they carry the substance of expression. They actually *communicate* something. Regulation of source code presents the converse of these cases. Whereas flag-burning involves meaningful expression without the form of speech, source code provides the form of speech without meaningful expression.[18]

Why did the Sixth Circuit ignore these core principles in *Junger* and adopt a remarkably expansive interpretation of the First Amendment in cyberspace? It did so because the court viewed source code using the close-up paradigm of what the code looked like, rather than the deeper functional perspective of what the code was actually supposed to do. Professor Junger's source code reprinted in an appendix must have appeared to the judges to be just like a speech in a quasi-foreign language, and it must have seemed natural to extend the same First Amendment protection to expression in a computer language that they would extend to expression in a foreign language. In other words, the court focused on the form of the speech, not its substance. Because

15. *See* City of Dallas v. Stanglin, 490 U.S. 19, 25 (1989) ("It is possible to find some kernel of expression in almost every activity a person undertakes – for example, walking down the street or meeting one's friends at a shopping mall – but such a kernel is not sufficient to bring the activity within the protection of the First Amendment.").

16. *See* Texas v. Johnson, 491 U.S. 397, 406 (1989).

17. *See* Buckley v. Valeo, 424 U.S. 1, 39-59 (1976).

18. Put another way, the fact that source code looks like speech should no more entitle source code to protection than the fact that burning a flag does not look like speech should disqualify flag-burning from protection.

the nuts-and-bolts of the source code looked like speech, the *Junger* court assumed that it was.

But this view hides a key assumption: that the close-up perspective of computer code offers the most appropriate means of determining how much protection code deserves as expressive speech. After all, the test for whether something constitutes protected expression is highly contextual; it depends on "the factual context and environment in which it was undertaken."[19] Walking down a street on your way to work would not be expressive for First Amendment purposes, but walking down the same street in a parade for civil rights certainly would be. Asking the abstract question of whether walking constitutes expressive speech looks at the wrong level of generality: the proper query is, in what particular circumstances is walking expressive? Similarly, the abstract question of whether source code constitutes expressive speech asks the wrong question; it fails to look at source code from the deeper perspective that would reveal constitutionally meaningful forms of expression.[20]

Just as viewing a Seurat painting from inches away reveals only dots, the *Junger* court's myopic view of source code revealed only communications that looked like speech in form, but lacked the deeper significance required to establish constitutional expression. By viewing code based on what it is rather than what it is designed to do, the *Junger* court was led to adopt a blanket rule that extended far greater protection to code in cyberspace than its equivalent receives in the physical world.

II. Patent Law

To qualify for patent protection, a new invention must fall within one of the specific categories that the Patent Act deems patentable subject mat-

---

19. Spence v. Washington, 418 U.S. 405, 410 (1974).

20. From this perspective, a useful starting point is to consider how much the First Amendment protects input delivered to machines. We frequently enter input into machines to instruct them to do what we want: some machines are configured to accept physical inputs (such as a car, which is driven by pressing and releasing foot pedals and turning a steering wheel), whereas other machines are configured to accept text inputs (such as a computer, which is instructed by source code converted to object code). The fortuity of how the machine is configured should not determine the degree of constitutional protection these inputs receive. This problem should become clear in several years when machines that today accept only physical inputs are reconfigured to accept text inputs. For example, it may be possible in the future to drive a car using speech, rather than through physical inputs such as a steering wheel. A driver might simply say, "Car, turn left on Pine Street and accelerate to fifty miles per hour." Should these instructions receive enhanced protection simply because they take the form of speech? Today, we understand the difference between writing a prose explanation for how to drive a car at illegal speeds and actually doing so: the former is protected speech, the latter an unprotected act that can lead to a ticket. Decisions such as *Junger* threaten to collapse this distinction. If drivers commit speeding offenses by telling their cars to accelerate to illegal speeds, will speeding laws violate the First Amendment?

ter.[21] The two most common categories, and the ones most relevant to Internet law, are "machines" and "processes." Most people intuitively understand machine inventions; Alexander Graham Bell's telephone and Thomas Edison's lightbulb provide classic examples. Patents for processes are no less important, however, because relatively few inventions take their full form in a tangible machine. For example, an inventor can obtain a process patent for a new way of refining oil, a new way of manufacturing industrial diamonds, or a new way of recycling plastics. These inventions discover new ways of manipulating preexisting materials to create new materials, or to create old materials in new ways. Patent law recognizes the importance of these inventions by extending patent protection beyond mere machines to cover processes as well. So long as the process satisfies the Patent Act's remaining standards of patentability, such as novelty, nonobviousness, and utility, then the process may be patented. After the process or machine is patented, the owner of the patent has a right to exclude others from making or using the invention for twenty years.[22]

The Patent Act's limitations on patentable subject matter prompt an obvious question in the Internet age: Can a computer program be patentable subject matter, and if so, when? The Federal Circuit offered its answer to this question in the landmark decision of *State Street Bank & Trust Co. v. Signature Financial Group*.[23] *State Street* involved a patent on a computer program that performed various specialized accounting functions. The program calculated incremental additions and subtractions to numbers that represented money held in pooled mutual funds and then outputted net gains, a final share price, and various other financial information that could be relied upon by financial analysts and regulators. Valuable stuff, the costly litigation suggests, but was it patentable? The Federal Circuit concluded that it was. A computer running a program is a "machine," the court reasoned, and it might even be a "machine" that executes a "process."[24] Further, it was a machine that produced "a useful, concrete, and tangible result," namely the output of the program, which in the

21. The invention must be "[a] process, machine, manufacture, or composition of matter, or . . . improvement thereof." 35 U.S.C. § 101 (1994).

22. *See* 35 U.S.C. § 154 (1994) (providing that patent term begins on "[the] date on which the patent issues and ending 20 years from the date on which the application for the patent was filed in the United States").

23. *See* State St. Bank & Trust Co. v. Signature Fin. Group, 149 F.3d 1368, 1372 (Fed. Cir. 1998).

24. *Id.* at 1372. Oddly, the *State Street* court seemed unconcerned with whether the invention at issue was a machine, or instead a process. After noting that the patent itself claimed that the invention was a machine, the Court refused to scrutinize the claim, stating simply that "for the purpose of a § 101 analysis, it is of little relevance whether [the claim] is directed to a 'machine' or a 'process,' as long as it falls within at least one of the four enumerated categories of patentable subject matter, 'machine' and 'process' being such categories." *Id.*

case of the *State Street* program was the final share price of the pooled funds.[25] Therefore, the computer program fell within the scope of patentable subject matter.

State Street teaches that every computer program is a "machine" that executes a "process," no matter what the program is or does. So long as the program creates an output, which essentially all programs do, it produces "a useful, concrete, and tangible result" and may be patented. No exceptions. This sounds a lot like *Junger*, doesn't it? Just as the Sixth Circuit in *Junger* indicated that all code is protected speech, the Federal Circuit in *State Street* indicated that all code is patentable subject matter. Just as code's status as code made it speech in *Junger*, code's status as code made it fall within the scope of patentable subject matter in *State Street*. Internet companies rushed to apply for patent protection.[26]

But does the result in *State Street* make any sense? Its holding certainly represents a dramatic expansion of the scope of patentability beyond what inventors have grown used to in the physical world. Before *State Street*, it was a fundamental axiom of patent law that any patentable invention had to rest on some interaction with realspace, with the natural world of physics, chemistry, and biology.[27] What distinguished patentable inventions from merely interesting ideas was that the former announced a new way that the natural world of realspace could be manipulated to reach a practical result. For example, you could patent a new design for a toothbrush; the toothbrush harnessed the laws of physics to manipulate the physical world and clean your teeth. On the other hand, you couldn't patent the idea of brushing your teeth; the idea was simply a conceptual advance that did not depend on any interaction with the physical world.

The rule announced in *State Street* flips that axiom on its head. Under *State Street*, an idea programmed as code and run on a computer ceases to be an idea and instead becomes a patentable "process" run on a "machine." The result is a strange dichotomy between "processes" run on the "machine" of a computer (which are patentable) and the "processes" run on the "machine" of the human brain (which are not). Take the accounting program patent at issue in *State Street*. The patent teaches a method, an algorithm for making a series of calculations. In theory, a very patient person could perform that series of calculations in his head; the laws of physics, chemistry, or biology need not

---

25. *See id.* at 1373 (quoting *In re* Alappat, 33 F.3d 1526, 1544 (Fed. Cir. 1994)).

26. *See, e.g.*, Raymond Van Dyke, *Software Patents Offer Opportunities and Obstacles: 'State Street' Sparked a Boom in PTO and Court Filings, and the Dust Has Not Quite Settled*, NAT'L L.J., May 24, 1999, at C19 ("As the aftershock of *State Street* subsides, the avalanche of new software patent issuances and litigation begins.").

27. *See* Gottschalk v. Benson, 409 U.S. 63, 66 (1972) (stating that inventions based on discovered law of nature must apply law of nature to new and useful end to be patentable).

apply. But if we found such a John Doe and taught him how to do the calculations, could we patent the method? Could we argue that John's brain is a patentable "machine" that executes a "process" and that we should have a right to enjoin anyone else from performing those calculations without paying us royalties? Of course not. You can't patent mere ideas. But switch the central processing unit from a human neural network to a silicon wafer and *voila!*, it's patentable.[28]

What explains the Federal Circuit's overprotection of code in *State Street*? The key is the court's embrace of a close-up perspective of computers and the virtual world of cyberspace. The *State Street* court envisioned computers as machines that process streams of instructions to create an output. From this perspective, it seems at least plausible to extend the reach of the patent laws broadly throughout the networked computers of cyberspace; after all, "machines" and "processes" are two categories of patentable subject matter. However, viewing cyberspace as just machines and processes is like viewing a Seurat painting as just dots; it misses the purpose of the entire enterprise. This close-up perspective ignores the virtual world of cyberspace that computers create, in which code defines every aspect of life ranging from trips to the store, the movies, and town square, to interactions in the bedroom and in politics.

From this deeper perspective, awarding patents to computer programs simply because they run on "machines" means that almost every aspect of life in cyberspace can be patentable subject matter. The result is that the patent laws can cover far more in cyberspace than they can in realspace. If someone devises a new way to shop for books, to conduct an auction, or to travel between different sites on the Internet, he can now obtain a patent that prevents the hundreds of millions of other users of the Internet from doing the same unless they pay him royalties.[29] Such restrictions on everyday life would be unimaginable in realspace, but *State Street* has made them routine in cyberspace. Instead of carving out the same sphere of unpatentable public domain that exists in realspace for cyberspace, the *State Street* court embraced a close-up view of computers and the Internet that led to a broad rule that extends far greater patent protection to cyberspace.

---

28. *Cf.* John R. Thomas, *The Patenting of the Liberal Professions*, 40 B.C. L. REV. 1139, 1160 (1999) ("After *State Street*, it is hardly an exaggeration to say that if you can name it, you can claim it.").

29. A famous example of such a patent is Amazon.com's one-click shopping patent. *See* Amazon.com, Inc. v. Barnesandnoble.com, Inc., 73 F. Supp. 2d 1228, 1232 (W.D. Wash. 1999) (enjoining defendant from using Amazon's patented "one click" method of placing product orders over Internet).

III. Electronic Privacy

The law of electronic privacy provides the third example of how Internet law overprotects code. The problem here is a statutory scheme, not a judicial decision. However, the analytical framework echoes the Sixth Circuit's approach to the First Amendment in *Junger* and the Federal Circuit's approach to patent protection in *State Street*. Once again, we find law that extends protection to code based on the nuts and bolts of what it is, rather than the broader picture of what it does.

To understand how privacy law can overprotect code in cyberspace, it helps first to understand the difference between the legal regimes that protect privacy against government monitoring in realspace and in cyberspace. In realspace, the primary source of protection against government monitoring is the Fourth Amendment.[30] The Fourth Amendment protects citizens from warrantless governmental invasions of their "reasonable" or "legitimate" expectations of privacy. This is a notoriously fact-sensitive standard; it permits the government to invade subjective expectations of privacy in some cases, but not others.[31] For example, government agents can watch us walk down a public street, but cannot break into our house to watch us sleep in our bed at night. Whether the government can watch you without a warrant depends on the context of where you are, of who you are, and of what you are doing.

Not so in cyberspace. In cyberspace, the primary source of protection against government monitoring is the federal statute known as the Wiretap Act, or "Title III."[32] Title III is considerably broader than the Fourth Amendment; it confers privacy rights on all parties to "electronic communications" regardless of what the communications happen to be or what message they contain. Because nearly every communication sent over the Internet is an "electronic communication,"[33] the result is a strikingly broad privacy scheme that prohibits real-time interception of essentially all Internet communications. Some exceptions do exist, of course. The government may intercept communications if a party to the communication consents,[34] and a network system administrator can intercept communications when it is a "necessary incident" to the protection of the network.[35] However, none of the exceptions to Title

30. U.S. CONST. amend. IV.

31. *See* O'Connor v. Ortega, 480 U.S. 709, 715 (1987).

32. 18 U.S.C. § 2510-22 (1994).

33. 18 U.S.C. § 2510(12) (1994). Some Internet communications carry the human voice; these communications are "wire communications" pursuant to 18 U.S.C. § 2510(1). Like electronic communications, wire communications receive the same statutory protection regardless of their contents.

34. *See* 18 U.S.C. § 2511(2)(c) (1994).

35. *See* 18 U.S.C. § 2511(2)(a)(i) (1994).

III take into account the nature or contents of the communications themselves. Instead, the status of the communication *qua* communication triggers the statutory protection against interception.

The failure of Title III to distinguish between different types of Internet communications creates bizarre results in practice. Consider the privacy rights of computer hackers who commit electronic trespasses onto the private networks of others. A hacker who breaks into a computer network should have no reasonable expectation of privacy in his activity within the victim network; like any other trespasser, he cannot object on constitutional grounds if the police watch as he commits his crime.[36] The statutory privacy protection of Title III draws no such nuanced distinction, however. Title III extends the same privacy protection to a computer hacker trying to take down a network as it does to an authorized user writing a personal note to his mother.[37] As a result, the statute gives hackers a privacy right in their attacks; unless an exception to the statute applies, Title III prohibits private parties or the government from even watching the crime occur. It is worth savoring the irony here. By failing to distinguish between authorized and unauthorized communications, Title III extends privacy protections to criminal efforts to invade the privacy of others. The computer hacker's undeserved statutory privacy right trumps the legitimate privacy rights of the hacker's victims.[38]

---

36. *See* United States v. Seidlitz, 589 F.2d 152, 160 (4th Cir. 1978) (suggesting that computer hacker has no reasonable expectation of privacy inside victim network); *see also* Rakas v. Illinois, 439 U.S. 128, 143 n.12 (1978) (noting that burglar "plying his trade" does not have reasonable expectation of privacy in victim's house during commission of burglary); Amezquita v. Colon, 518 F.2d 8, 11 (1st Cir. 1975) (holding that trespassers cannot establish reasonable expectation of privacy on government land).

37. This effect is ameliorated somewhat by the fact that unauthorized users probably do not have standing to move for suppression of illegally intercepted communications because no actual privacy interests were invaded. *See* Scott v. United States, 436 U.S. 128, 139 (1978) (suggesting that standing to move for suppression under Title III mirrors standing under Fourth Amendment); United States v. Baranek, 903 F.2d 1068, 1072 (6th Cir. 1990) (same); *Seidlitz*, 589 F.2d at 160 (expressing "serious doubts" as to whether computer hackers have standing to move for suppression of illegally intercepted communications). Of course, this distinction itself has little meaning given that Title III presently does not contain a suppression remedy for the unauthorized interception of intercepted electronic (as opposed to oral or wire) communications; instead, the primary remedy is civil damages. *See* Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 461 n.6 (5th Cir. 1994).

38. The remarkable results that this scheme produces are illustrated by a recent case involving a "cloned" cellular phone, which is a cell phone illegally programmed with the stolen access numbers of a legitimate phone to provide the owner of the cloned phone with free cellular service. In *McClelland v. McGrath*, 31 F. Supp. 2d 616 (N.D. Ill. 1998), police officers investigating a kidnaping traced the kidnaper's telephone calls to a cloned cellular phone. Eager to learn more about the kidnaper's identity and location, the police asked the cellular provider to intercept the kidnaper's communications and relay any information to the officers that might permit them to find the kidnaper and save his victim. The provider complied, and the provider's

How did we arrive at such a strange result? Here, a page of history is worth a volume of logic. Congress enacted Title III in 1968 following two Supreme Court decisions interpreting the Fourth Amendment: *Berger v. New York*,[39] which announced Fourth Amendment limits on wiretapping phone lines,[40] and *Katz v. United States*,[41] which found Fourth Amendment problems in the use of electronic listening devices commonly known as "bugs."[42] As passed in 1968, Title III prohibited the use of devices to intercept two types of communications: "oral communications,"[43] which were defined as conversations that supported a reasonable expectation of privacy (thus prohibiting the use of privacy-invading bugs in response to *Katz*), and "wire communications,"[44] which were conversations carried by wire (thus prohibiting telephone wiretapping in response to *Berger*). Notably, the definition of "wire communications" did not include the requirement that the communications support a reasonable expectation of privacy. This would have been superfluous; in 1968, all wire communications were human-to-human telephone conversations that seemed intrinsically private.[45]

When Congress amended Title III in 1986 and added a third category of communications to the statute to include Internet communications, it chose to model the new third category, "electronic communications," on the structure of the second category, "wire communications."[46] This was a reasonable judgment at the time; it made sense to protect data in the same way that the statute protected voice.[47] As a result, the definition of "electronic communications" did not incorporate any requirement that the communication should be

---

information led the police to the kidnaper. After being caught, the kidnaper brought a civil suit against the police alleging that their actions directing the provider to intercept his unauthorized calls violated his statutory privacy rights. The district court agreed. *Id.* at 619.

39. 388 U.S. 41 (1967).

40. Berger v. New York, 388 U.S. 41, 62-63 (1967).

41. 389 U.S. 347 (1967).

42. Katz v. United States, 389 U.S. 347, 359 (1967).

43. 18 U.S.C. § 2510(2) (1994).

44. 18 U.S.C. § 2510(1) (1994).

45. In fact, the legislative history of Title III indicates that Congress was attempting to track the Fourth Amendment when it extended privacy protections to all parties to telephone conversations, regardless of the contents of those communications. *See* S. REP. NO. 90-1097, at 96 (1968).

46. *See* H.R. REP. NO. 99-647, at 34-35 (1986) (explaining source of definition for "electronic communication"). *Compare* 18 U.S.C. § 2510(12) (1994) (defining electronic communications) *with* 18 U.S.C. § 2510(1) (1994) (defining wire communications).

47. Interestingly, Title III does not treat data and voice entirely equally. For example, the unauthorized interception of data does not trigger a suppression remedy, whereas interception of voice does result in suppression. *See* 18 U.S.C. § 2518(10)(a) (1994); Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 461 n.6 (5th Cir. 1994).

able to support a reasonable expectation of privacy. Every electronic transfer of data, "of any nature,"[48] constituted a protected electronic communication.

Whether protecting all Internet communications equally made sense in 1986, it certainly makes no sense today. Today we realize that Internet communications mirror the extraordinarily rich and diverse offerings of cyberspace. If you were to select a random spot on the Internet and watch the Internet traffic streaming by, you would pick up e-mails, Web pages in transit, commands sent to remote servers, picture or music files, network support traffic, and almost everything else in cyberspace. Many of these communications would deserve privacy, but others would not. Much like human behavior in realspace, electronic behavior in cyberspace is too varied to fit within a single paradigm. One-size-fits-all doesn't work.[49]

Title III's regime for protecting Internet communications from interception thus suffers from the same problem that the Sixth Circuit encountered in *Junger* and the Federal Circuit encountered in *State Street*. By adopting a myopic view of the Internet that focuses on the nuts-and-bolts of what it is rather than on the virtual world that the Internet creates, Title III paints with a brush so broad that it encompasses all code. Every bit and byte qualifies. The close-up perspective reveals only dots, and fails to recognize the important distinctions among the different kinds of communications in cyberspace.

IV. Conclusion

The purpose of this Essay has been to critique a way of thinking about Internet regulation. I have focused on judicial decisions and a statutory scheme that regulate Internet code without considering its contents, and have suggested that this nuts-and-bolts, close-up approach to the Internet lacks nuance and tends to overprotect code compared to its equivalents in the physical world. By making this argument, however, I am not suggesting that the close-up view of the Internet will *never* provide an effective way of regulating cyberspace. Both law and cyberspace are too diverse for a single perspective to work every time. However, I am suggesting that the close-up view of the Internet will often prove inadequate. Most legal doctrines draw distinctions based on function, not form, and we should strive to maintain these distinctions when applying traditional legal doctrines to the new world of the Internet. The deeper perspective of cyberspace that focuses on function rather than form will usually provide the best way of translating our doctrines and our values from the physical world to a virtual one.

---

48. 18 U.S.C. § 2510(12) (1994).

49. *See* Wu, *supra* note 7, at 1163 ("A singular model of Internet usage has become too small to capture the dramatic diversity of today's Internet.").

NOTES